Extraterritorial Application of the USA PATRIOT Act and Related Regimes: Issues for European Banks Operating in the United States

ROBERT J. GRAVES AND INDRANIL GANGULI

The authors review the background and scope of the USA PATRIOT Act and discuss the interplay of the anti-money laundering statutes and regulations and the combat of terrorist financing provisions with the U.S. financial sanctions regimes. The authors also highlight the resulting legal issues affecting the business operations of foreign banks, especially those headquartered in the Member States of the European Union with substantial business interests in the United States, and explain that the issues largely center around correspondent account transactions and clearing issues as well as home and host country compliance conflicts resulting from significant differences between EU and U.S. boycott and data protection regimes.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)[1], passed hastily by the United States Congress in response to the terrorist attacks on September 11, 2001, reflects the effort of the U.S. government to heighten the international response to the financing of terrorist activities. In volume and breadth, the legislation is enormous. Its most fundamental aim is to increase the amount and quality of information available to U.S. authorities responsi-

Published in the October 2007 Privacy & Data Security Law Journal.

ble for preventing terrorism and other criminal activities. To this end, the Act expands the allowable methods of information gathering, improves information sharing among government agencies, and increases funding for certain intelligence projects. Additional measures enhance border security, tighten entrance and visa requirements, and strengthen the criminal laws against terrorism.

The banking provisions of the USA PATRIOT Act are a significant addition to the existing legal framework established by the Bank Secrecy Act (BSA), various executive orders[2] issued by the President of the United States and the designations of the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury (DoT).[3] Together, these have created considerable pressures on foreign banking institutions — with or without a business presence in the United States — to comply with U.S. programs, including "smart" financial sanctions, anti-money laundering (AML) statutes and regulations, and the combat of terrorist financing (CFT).[4] Such pressures have resulted in a steady increase in the intensity and extraterritorial reach of U.S. regulations. Additionally, the various U.S. programs provide the legal basis to enforce, if necessary, tough punitive and supervisory measures against foreign banks depending on the severity of violations assessed by the responsible U.S. federal and state agencies.[5]

In addition to reviewing the background and scope of the USA PATRIOT Act, this article also discusses the interplay of the AML/CFT provisions with the U.S. financial sanctions regimes. The article highlights the resulting legal issues affecting the business operations of foreign

Robert J. Graves is a partner in the Chicago office of Jones Day, where he is the firmwide co-chair of the Banking & Finance practice. He can be reached at rjgraves@jonesday.com. Indranil Ganguli is a division manager in the Association of German Public Sector Banks (Bundesverband Öffentlicher Banken Deutschlands) in Berlin, Germany, where he works with issues relating to banking supervision, anti-money laundering regulations, financial sanctions, and foreign trade. He can be reached at indranil.ganguli@voeb.de. The authors wish to thank J. Barrett Ellis, an associate in the Chicago office of Jones Day, for his assistance in the preparation of this article.

banks, especially those headquartered in the Member States of the European Union (EU) with substantial business interests in the United States (i.e., EU banks).[6] The article explains that the issues largely center around correspondent account transactions and clearing issues as well as home and host country compliance conflicts resulting from significant differences between EU and U.S. boycott and data protection regimes. These issues and conflicts are highly complex, but nevertheless very relevant for foreign and especially EU banks conducting business transactions denominated in U.S. Dollars.

TITLE III USA PATRIOT ACT AND THE SCOPE OF U.S. AML REGULATION

Although the scope of the USA PATRIOT Act is expansive, foreign banking institutions should be concerned primarily with Title III, which amends the BSA and authorizes expansion of U.S. AML regulation.[7] Title III originates from the U.S. Congress's concerns regarding the ease with which terrorists and money launderers were able to manipulate offshore facilities, correspondent accounts, and institutions within weak regulatory regimes. Title III formally recognizes that preexisting regulations were growing outmoded and states updating money laundering control as its express purpose. Title III strengthens existing law to hinder the funding of terrorism and criminal activities and to assure access to the identities of the real parties in interest to financial transactions.

Title III vests responsibility for promulgating regulations to support the statute in the Secretary of Treasury and provides the Secretary with broad discretion and authority to implement this legislative mandate. Specific provisions provide for:

- Due diligence requirements for U.S. financial institutions that maintain correspondent accounts for foreign banks;
- Enhanced due diligence for U.S. financial institutions providing correspondent accounts within jurisdictions or to institutions that are of special concern to the U.S. government;

- A general prohibition preventing U.S. financial institutions from maintaining correspondent accounts for foreign shell banks;
- Subpoena powers for the U.S. government over documents and information held at non-U.S. banks that maintain correspondent accounts with U.S. banks;
- Broad new authority for the U.S. government to seize the funds of foreign banks held in interbank accounts where tainted funds are deposited in the non-U.S. accounts of those banks; and
- Other measures requiring additional information regarding the dealings of U.S. banks in jurisdictions of special concern.

Title III expressly authorized Congress to rescind the operative provisions of the statute in 2005, but Congress chose not to do so. Many issues of the enforcement and administration of the USA PATRIOT Act are just now beginning to arise. The DoT did not promulgate a final rule governing due diligence requirements under the foreign correspondent account provisions of the Act until January 2006. Little precedent under the regulation exists. Furthermore, the government's seizure and subpoena powers under the Act may be exercised privately, and may not be a matter of public record.

One political and legal controversy that has unfolded over the past year demonstrates the difficulties and consequences of international enforcement of more exigent U.S. banking regulations promulgated in light of the perceived threat of terrorism. In July 2006, conflict arose when U.S. newspapers revealed a confidential surveillance program under which the U.S. government monitored the data related to large volumes of international financial transactions handled by the Society for Worldwide Interbank Financial Telecommunications (SWIFT).[8] SWIFT is a Belgium-based company with offices in the United States that operates a secure and standardized worldwide messaging system used to transmit, inter alia, bank transaction information by providing interface software to over 8,100 financial institutions in 208 countries and territories.[9] The precise locus of U.S. authority to issue the subpoenas was not initially clear. Later, it became evident that OFAC, operating on the basis of powers under the Terrorist Finance Tracking

Program (TFTP) served administrative subpoenas on SWIFT. These subpoenas required SWIFT to transfer personal data held on its United States server[10] to OFAC, where such data are used for counterterrorism purposes regarding suspected individuals or entities.

After these facts were unveiled by the media, a commission appointed by the Belgian Data Protection Authority[11] issued its opinion of September 27, 2006 stating that SWIFT processing activities for the execution of interbank payments and its compliance with the OFAC surveillance program violated Belgian data protection law, which implements the EU Data Protection Directive.[12] The Belgian Data Protection Authority found several breaches to the fundamental data protection principles, including those related to transfers of personal data to third countries. Moreover, a European panel[13] expressed doubts about the legality of SWIFT's actions.[14] SWIFT has maintained that it did no more than comply with U.S. subpoenas. However, the Belgian Data Protection Authority is now in discussions with SWIFT regarding appropriate compliance with Belgian data protection law.[15]

For non-U.S. institutions, compliance with the USA PATRIOT Act and OFAC regulations presents complex issues. As in the SWIFT controversy, European banks may face competing demands from U.S. and domestic jurisdictions. Accordingly, their actions must be informed by knowledge of U.S. statutes and regulations, as well as relevant provisions of European and home-country law. The generally more stringent privacy and data protection demands in European jurisdictions are particularly likely to create difficulty. At present, European banks wishing to maintain relationships with U.S. financial institutions must be prepared to provide increased information both to the banks they work with and to the U.S. government. In addition, European banks may wish to consider carefully their own customers to avoid contacts that could interfere with their relationships with U.S. financial institutions.[16]

PROVISIONS OF THE USA PATRIOT ACT AFFECTING FOREIGN BANKS

The primary changes to U.S. AML regulation wrought by the USA

PATRIOT Act are twofold: (1) expanded due diligence requirements and (2) broadened powers to seize and subpoena. In addition, there are new prohibitions on dealings with shell banks, as well as special measures that may be imposed on jurisdictions of concern.

Due Diligence

The USA PATRIOT Act requires that U.S. financial institutions that maintain a correspondent account in the United States for a foreign bank establish due diligence policies designed to detect money laundering activities in the account.[17] The promulgation of regulations under this statutory provision proved controversial, but a final rule emerged in January 2006.[18]

The Financial Crimes Enforcement Network (FinCEN) is the bureau of the DoT charged with promulgating rules under the AML provisions of the USA PATRIOT Act. FinCEN has broad powers under the Act to coordinate law enforcement, intelligence and data gathering with respect to financial crimes and money laundering. FinCEN initially proposed a rule under the USA PATRIOT Act's due diligence provisions that broadly defined correspondent accounts and described specific steps for due diligence.[19] The rule was heavily criticized as too broad in its definitions and too prescriptive in its requirements. Although the final rule maintained the expansive definitions, it did allow for a more relaxed, risk-based approach to due diligence.

Banks should be aware that the definition of "correspondent account" under the USA PATRIOT Act and DoT regulation is considerably broader than trade usage. FinCEN opted to retain the statutory definition, which begins with any account "…established to receive deposits from [and] make payments on behalf of a foreign financial institution." Although this description is consistent with commonly understood trade usage, the definition continues, drawing in accounts intended to "handle other financial transactions related to" foreign financial institutions.[20] This final language is sufficiently broad to encompass most formal banking relationships between U.S. and foreign banks.

The risk-based approach prescribed by regulation requires U.S. financial institutions to weigh several factors prior to proceeding with due dili-

gence for a foreign bank correspondent account. Banks are first to consider whether the account might be subject to enhanced due diligence (see below). They must then determine the money laundering risk posed, giving consideration to five factors:

- The nature of the foreign institution and its market;
- The type, purpose, and activity of the account;
- The nature and duration of the relationship of the foreign institution with the U.S. financial institution;
- AML regulations and supervision in the foreign jurisdiction;
- Obtainable information regarding the foreign institution's anti-money laundering record.[21]

Once the correspondent account has been assessed, the bank must apply appropriate procedures and controls. The account must then be periodically reviewed to determine that information obtained during due diligence is consistent with the type, purpose, and activity of the account.

Non-U.S. banks can garner at least three insights from the regulation. First, home-country rules are important. The AML regulations of a bank's home jurisdiction will play a key role in determining the vigor of the due diligence with which it must comply. Second, the banks' own internal policies are highly relevant. Stringent money laundering detection programs will provide assurance to U.S. banks, limiting more intrusive review. Finally, banks should be aware of their customer base. Even though U.S. banks may not directly confront the customers of a correspondent account holder, those customers can affect the banks' risk assessment for the account.

Enhanced Due Diligence

For certain correspondent accounts held by foreign banks, U.S. financial institutions must conduct enhanced due diligence.[22] Under the USA PATRIOT Act, such due diligence must occur where the account is maintained by a foreign bank operating under an offshore banking license or

under a banking license issued by a country or territory that has been designated by the Paris-based Financial Action Task Force on Money Laundering (FATF)[23] as non-cooperative (so called NCCTs)[24] with international AML principles or as warranting special measures due to money laundering concerns.

Like the rule governing ordinary due diligence, the enhanced diligence rule takes a risk-based approach, though certain threshold measures are required regardless of risk.[25] Pursuant to the regulation, U.S. banks must conduct "enhanced scrutiny" that "reflect[s] the risk assessment of the account." Enhanced scrutiny includes, as appropriate, obtaining information about the foreign bank's anti-money laundering programs, monitoring transactions to, from, or through the correspondent account and identifying persons with authority to direct transactions through any account that is a payable-through account. U.S. banks must determine the identity of any person who owns or controls more than 10 percent of any foreign bank that is not publicly traded. Finally, U.S. banks must ascertain whether the relevant foreign bank provides correspondent accounts to other foreign banks. If the foreign bank maintains such accounts, the U.S. bank, giving consideration to risk, must take appropriate measures to "assess and mitigate" risk associated with the foreign bank's correspondent accounts with other foreign banks.

This final requirement raises an important issue. Officials and commentators have expressed concern with "nesting" accounts. Although the U.S. government attempts indirectly to regulate foreign banks through their dealings with U.S. entities, the government worries that money laundering activities will simply move into accounts of banks that deal with other foreign institutions who themselves hold correspondent accounts with U.S. banks. A suspicious account would thus "nest" in another account, staying a step away from U.S. regulation and detection. The final requirement of enhanced due diligence attempts to address this problem. Further efforts to contend with nesting are evident in the prohibition on shell banks, which will be discussed below. Even where there are not direct measures aimed at nesting, non-U.S. banks may wish to be aware of the concern, recognizing that compliance will be easiest if even accounts unrelated to correspondent accounts are free from suspicion. As

noted above, the internal policies of a foreign bank and the financial regulatory regime of the bank's home country will affect the nature of due diligence conducted by U.S. banks.

Measures for Jurisdictions of Primary Money Laundering Concern

Where the Secretary of the Treasury has special concerns regarding a jurisdiction, an institution, or a class of transactions, the Secretary may require that involved U.S. banks take one or more of five special measures created by statute.[26] Those measures are:

- Recordkeeping and reporting of financial transactions identified by the Secretary of the Treasury, reported in a form and maintained for a duration the Secretary prescribes, and including, but not limited to, the identity of the participants of a transfer, the legal capacity in which a participant acts, the identity of the beneficial owner of funds, and a description of the transaction.
- Maintaining information related to beneficial ownership of any U.S. accounts opened or maintained by a foreign person.
- Maintaining information, including the identity of each customer and other information generally obtained in the U.S. at the opening of a deposit account, relating to payable-through accounts identified by the Secretary of the Treasury as being of primary money laundering concern.
- Maintaining information, including the identity of each customer and other information generally obtained in the U.S. at the opening of a deposit account, relating to correspondent accounts identified by the Secretary of the Treasury as being of primary money laundering concern.
- Prohibitions or conditions on opening or maintaining correspondent or payable-through accounts identified by the Secretary of the Treasury as being of primary money laundering concern.[27]

In choosing which measures are appropriate, the Secretary of the Treasury must consult with the Chairman of the Federal Reserve, the Secretary of State, the Securities and Exchange Commission, and the National Credit Union Administration Board. Additionally, the Secretary of the Treasury may choose to confer with other appropriate agencies. The statute requires that the Secretary consider actions taken by other nations or multilateral groups, cost and competitive disadvantage in the U.S., systemic impact, and the effect of the contemplated measures on U.S. national security and foreign policy.

A finding of "primary money laundering concern" is made by the Secretary of the Treasury in consultation with the Secretary of State and the Attorney General. Although the Secretary of the Treasury apparently has broad discretion in making his finding, the statute does provide guidelines and requires assessment of both (1) jurisdictional and (2) institutional factors.

1. Jurisdictional factors include:
    - The presence of high-risk groups and the extent of bank secrecy offered to nonresidents of the jurisdiction;
    - The volume of transactions in proportion to the size of the economy of the jurisdiction;
    - The experience of U.S. law enforcement in obtaining information in the jurisdiction; and
    - Institutional corruption within the jurisdiction.
2. Institutional factors include:
    - The extent to which institutions are used to promote money laundering in the jurisdiction; and
    - The extent of the legitimate use of institutions within the jurisdiction.[28]

EU banks should be mindful of the possibility of special measures, although banks in larger, well-regulated economies will likely remain untouched. The current list of targeted institutions and jurisdictions is short. Burma and Syria, along with institutions within their jurisdiction, are subject to special

measures. A final rule was issued in April 2007, imposing measures against Banco Delta Asia and two of its subsidiaries. Proposals are currently pending regarding institutions in Belarus and the so-called Turkish Republic of Northern Cyprus. Within the EU, only two Latvian banks have been subject to scrutiny. A proposal imposing measures with respect to Multibanka in Latvia was withdrawn after FinCEN expressed confidence in measures taken by the Latvian government, including steps to comply with the EU Cash Control Regulation.[29] The bank also took measures, closing 98 percent of its foreign accounts. A final regulation remains effective, however, against VEF Banka in Latvia. Despite the U.S. government's increased comfort with Latvian regulation, the VEF Banka has not taken sufficient internal measures to avoid scrutiny.

Prohibition on Correspondent Accounts with Foreign Shell Banks

The USA PATRIOT Act prohibits U.S. banks from maintaining correspondent accounts with foreign shell banks (banks that do not have a physical presence in any country).[30] The related FinCEN regulations[31] make significant substantive additions to the statute. As in the regulations governing due diligence requirements, the definition of "correspondent account" is broader than in typical usage. FinCEN did, however, clarify that most isolated or occasional transactions with foreign banks did not fall under the definition, easing fears that almost any transaction could give rise to a correspondent account for purposes of the shell bank regulation.

Under the FinCEN regulation, foreign branches of U.S. banks are not required to comply with the prohibition. The regulation also carves out an exception for accounts held by foreign banks that that are affiliates of a regulated institution. Otherwise, all U.S. banks must comply. As a safe harbor, U.S. banks may obtain a certification from foreign correspondent account holders. Recertification must be done every three years or more frequently if a bank knows, or has reason to know, that information in a certification is no longer correct.

U.S. banks must also take "reasonable steps" to assure that correspondent accounts maintained for a foreign bank are not used indirectly to

provide banking services to a foreign shell bank. Again, this requirement is born out of concern with nesting accounts, underlining the U.S. government's concern that foreign terrorists and criminals will access U.S. financial institutions through other foreign entities. Non-U.S. banks will wish to be wary of their own customers to avoid interference with their relationships to U.S. banks.

JURISDICTION, SUBPOENA, AND SEIZURE ISSUES

The US has long employed freezes and blocks of U.S. Dollar transfers, even transfers occurring outside of its borders, to accomplish foreign policy aims.[32] The USA PATRIOT Act expands U.S. jurisdiction over foreign persons, increasing U.S. power to employ these tools to an extent that foreign financial institutions may find troubling. The U.S. government in many instances cannot directly impose sanctions on foreign persons or institutions suspected of money laundering or harboring and encouraging international terrorism. Where the government cannot do so, the USA PATRIOT Act broadens the government's power to sanction the intermediaries used by foreign persons and institutions to access U.S. markets. Cooperation with due diligence and compliance with subpoenas is necessary if a bank wishes to conduct business regularly with a U.S. financial institution. Furthermore, the USA PATRIOT Act has created unprecedented seizure powers over funds held in the United States, giving it effective power over funds held abroad.

The Limited Jurisdiction of OFAC and PATRIOT Predecessors

Prior to enactment of the USA PATRIOT Act, the Office of Foreign Assets Control (OFAC) was the center of action against foreign terrorists, narcotics traffickers, and money-launderers. OFAC is an office within the DoT charged with coordinating U.S. sanctions programs. Such programs are the result of specific legislation and various executive orders of the President of the United States. Many sanctions maintained by OFAC are multilateral in scope, stemming from United Nations and other international mandates. Others, however, are specific to U.S. interests.

One of the primary sources for OFAC regulation is the International

Emergency Economic Powers Act of 1977 (IEEPA). IEEPA gives the President of the United States special wartime and national emergency powers pursuant to which the President can declare a national emergency and order appropriate sanctions against foreign persons, entities, or nations. The President exercises his authority through executive orders. Additional statutes, such as the Antiterrorism and Effective Death Penalty Act, delegate authority to the Secretary of the Treasury to establish sanctions against foreign persons or entities. From these programs, OFAC creates the Specially Designated Nationals (SDN) List. The SDN list contains over 3,500 names of individuals or entities connected to the various OFAC sanctions programs.

OFAC regulations apply to all U.S. persons, including foreign branches of U.S. banks, and, in certain cases, U.S. bank subsidiaries located abroad. Two limitations, however, are notable. First, although OFAC regulations apply to all U.S. persons, they do not prescribe specific compliance regimes. Individuals, companies, and financial institutions are left broad discretion to design and implement their own compliance programs. As discussed above, USA PATRIOT Act regulations have backed away from overly prescriptive compliance regulations, but nonetheless go far in describing the steps that institutions must take to achieve the USA PATRIOT Act's objectives. Second, the jurisdiction exercised by OFAC, while expansive on a national level, hews closely to the traditional limits of the jurisdiction of the government of a sovereign state in the international sphere.

OFAC regulations thus do not create a direct threat of legal action against foreign financial institutions that are not also U.S. persons. As discussed below, the USA PATRIOT Act does create the possibility of such action. Foreign financial institutions will encounter OFAC regulations only as they deal with U.S. institutions that must ensure their own compliance. As noted, OFAC regulations leave banks with greater flexibility to develop their own compliance measures, and so problems of competing legal requirements may be solved more easily than such problems created by the USA PATRIOT Act.

Long-Arm Jurisdiction

The USA PATRIOT Act amends the federal statute governing laundering of monetary instruments to expand jurisdiction over foreign persons.[33] Under the amended statute, courts may exercise jurisdiction over foreign persons who commit a money laundering offense that involves a financial transaction in the United States. Jurisdiction may also be exercised if a foreign person converts property that has been subject to forfeiture by court order or if the foreign person is a financial institution that maintains a bank account at a U.S. financial institution. To ensure access to funds, the USA PATRIOT Act gives courts exercising the new long-arm jurisdiction authority to issue a restraining order whereby a receiver takes custody of the assets. Assets subject to this authority may be located either inside or outside of the United States.

Subpoena Powers

The USA PATRIOT Act authorizes the Secretary of the Treasury or the Attorney General to subpoena records from a foreign bank that maintains a correspondent account with a U.S. bank.[34] The records must relate to the correspondent account, but may be held outside the United States and may include information about deposits into the foreign bank. Under the USA PATRIOT Act, the U.S. bank that maintains the relevant correspondent account must terminate the account if the foreign bank fails to comply with the subpoena.

The Act permits foreign banks to initiate proceedings in a U.S. court to contest a subpoena. Instructive precedent for challenge has yet to emerge, however, and the sweeping new subpoena powers leave well-settled law in doubt. Particularly troubling will be instances in which disclosure would result in violation of home-jurisdiction laws. Already, European privacy and data protection laws present significant dilemmas. Historically, courts have undertaken a balancing test, considering the importance of U.S. and foreign interests, the specificity of the request, alternative means of securing the information, and the importance of the information to the relevant investigation. Whether this balancing test remains intact in USA PATRIOT Act actions is uncertain. Even presum-

ing that it does, the Act's antiterrorism purposes may cause courts consistently to find that the U.S. interest outweighs all other factors. If this is true, the inability to assert foreign interests against U.S. government-issued subpoenas will likely prove to be one of the most contentious issues in the anti-money laundering provisions of the USA PATRIOT Act.

Asset Forfeiture

The USA PATRIOT Act employs a legal fiction to give U.S. authorities seizure power over the funds of foreign banks held in U.S. interbank accounts.[35] If the U.S. government believes that illegal proceeds have been deposited in the foreign account of a foreign bank, it assumes those proceeds to have been deposited in an interbank account held in the United States by such foreign bank. The government may then seize the funds from the interbank account. It need not establish that the funds are directly traceable to funds deposited into the foreign financial institution from whose account they were seized.

There are two possibilities of relief from these provisions. First, forfeiture may be suspended by the Attorney General where a conflict of law exists and the suspension would serve justice and not harm the interests of the United States. Alternately, the "owner" of the targeted funds may institute an action under 18 U.S.C. § 983. In a Section 983 action, the government has the burden of demonstrating that the funds were subject to seizure. The owner of the funds may defend with a claim that it is an "innocent owner" by showing either that it did not know of the conduct giving rise to the forfeiture or that, upon learning of the conduct, it did all that could be expected to terminate it.

The statutory definition of "owner" contravenes the conventional understanding of banking relationships, which holds that the bank, upon receipt of a deposit, becomes the owner of the deposited funds and a debtor to the depositor.[36] Under the USA PATRIOT Act, only the owner of the funds "at the time such funds were deposited" may challenge a seizure. The definition specifically excludes the foreign bank that received the deposit, as well as any intermediary financial institution.[37] Two limited exceptions allow a foreign bank to make a claim if it is the accused wrongdoer or if it can establish that it had discharged its obliga-

tions to the prior owner of the funds.

A general savings clause found in Section 316 of the USA PATRIOT Act could allow a foreign bank subject to a seizure to make a Section 983 claim, although courts have not yet considered this possibility. Additional possible remedies are only more speculative. Conceivably, a court could find that a USA PATRIOT Act seizure violated Fourth Amendment protection against unreasonable search and seizure, Fifth Amendment protection against takings without just compensation, or more general constitutional principals of standing.[38] Ultimately, the status of a foreign bank's right to challenge a seizure is unknown, as instructive precedent has yet to emerge.

Bank Examinations; Expansion Activities

USA PATRIOT Act and AML compliance is a focus of U.S. bank examinations, and banks are increasingly expressing their concern that money laundering enforcement and penalties have become too onerous.[39] Failures to comply are more likely than most legal violations to result in formal enforcement actions, including substantial civil money penalties, against banks. Financial institutions who fail to terminate a correspondent account at the instruction of the Secretary of the Treasury, for example, are subject to a daily $10,000 penalty. Even harsher may be "no growth" restrictions imposed on banks deemed to be noncompliant. In addition, the USA PATRIOT Act expressly requires the U.S. bank regulators to consider the effectiveness of an acquiring bank holding company or bank in combating money laundering activities in the U.S. and their overseas branches. An institution acquiring a U.S. institution with a history of AML issues will have to demonstrate how it can and will cure these deficiencies.[40]

Penalties

Foreign banks with substantial business interests in the U.S. or that are maintaining funds in U.S. interbank accounts face considerable civil and criminal law risks if they are deemed by the U.S. authorities to have violated provisions of the AML or OFAC regimes. Moreover, U.S. citizens serving as senior or executive officers or members of the board of a

foreign bank may be confronted with criminal law charges and severe penalties if they are party to a foreign bank's board decisions concerning establishment of business relationships or transactions with counterparties unilaterally designated or sanctioned by the U.S. government. Section 353 intensified the problem by increasing civil and criminal penalties for violations of any orders made under the BSA. Civil and criminal penalties were also increased for violations of regulations prescribed under Section 21 of the Federal Deposit Insurance Act and Section 123 of Public Law 91-508.[41] Section 123 of Public Law 91-508 specifies regulations that govern recordkeeping for uninsured banks or institutions, or any other institution defined in 12 U.S.C. § 1953(b),[42] while Section 21 of the Federal Deposit Insurance Act specifies regulations that govern recordkeeping for insured depository institutions.[43] The section also lengthens the effective period of geographic targeting orders (e.g., against Cuba or Syria or persons domiciled in these countries) from 60 days to 180 days.[44] Furthermore, Section 363 gave the Secretary of the Treasury the authority to issue money penalties in an amount not less than two times the amount of the transaction, but not more than US$1,000,000 on any financial institution or agency that commits a civil[45] or criminal[46] violation of international anti-money laundering measures.[47]

SQUARING THE CIRCLE — ISSUES AND OPTIONS FOR EU BANKS

As discussed, the framework of AML/CFT regulations and the "smart" financial sanctions established by the BSA, the USA PATRIOT Act, the Presidential Executive Orders, and the designations of OFAC — as well as the interplay of these legal regimes — has created considerable pressures and risks for EU banks with or without a business presence in the U.S. to comply with U.S. regulations in an extraterritorial context, if necessary. Given the high political priority accorded by the U.S. government to AML/CFT issues after the 9/11 terrorist attacks, these compliance pressures seem likely to increase over time for all banking institutions in the U.S.[48] The pivotal issue for internationally active EU banks with substantial U.S. business interests remains the assessment of options to miti-

gate the compliance risks while conducting business in multiple jurisdictions. Additionally, they are confronted with civil law and privacy and data protection issues such as those that surfaced during the SWIFT controversy.[49] Therefore, they have developed a twofold approach to cope with the pressing issues: (1) adjusting their internal procedures and (2) lobbying the EU and its Member States for protection and requesting that the responsible U.S. government agencies provide some regulatory relief. The following sections demonstrate, however, that the approaches chosen by EU banks to safeguard their interests are far from optimal.

Dollar Clearing and Related Risk Mitigation and Civil Law Issues

EU banks confront a dilemma when they participate in the U.S. Dollar clearing system for payment and settlement of their cross-border transactions. They are required to comply with regulations and unilateral financial sanctions enforced within the jurisdiction of the U.S. that have no equivalent in the relevant laws and regulations of the United Nations (UN), the EU, or the home country authorities of the respective EU Member States in which they are headquartered. Therefore, EU banks —including those without a business presence in the U.S. — that are party to the U.S. Dollar clearing system face the risk of being penalized by measures such as asset freeze and seizure/forfeiture, subpoena, penalties, and enhanced supervision if they fail to comply with U.S. AML/CFT regulations or unilaterally imposed financial sanctions. The risk is substantial where EU banks are involved in ordinary trade and export finance transactions where:

- The customers are European exporters;
- The counterparties are importers domiciled in third countries who have not been identified as uncooperative by the authorities of the EU or the home country but unilaterally sanctioned by the U.S. government pursuant to Section 311 USA PATRIOT Act as persons or institutions of primary money laundering concern; and
- The funds in connection with the transaction are denominated in U.S. Dollars.

The U.S. government has on various occasions declared that the authorities exercise restraint in the use of their Section 319(a) powers. The enforcement actions against ABN AMRO Bank and Deutsche Bank, however, demonstrated that substantial asset seizure and forfeiture risks do exist for EU banks operating in the U.S. with regard to their funds deposited in the accounts of U.S. correspondent banks.[50] Whether EU banks in such situations have a sufficient basis for recourse to the parties on whose behalf they carried out the transactions at risk is also questionable. Moreover, conducting business transactions that involve risky counterparties by denominating the funds in Euros instead of U.S. Dollars does not solve the problem for EU banks, as long as the counterparties are regarded as individuals or institutions of primary money laundering concern by U.S. authorities. As mentioned earlier, funds connected to transactions involving counterparties identified as risky are subject to asset seizure and forfeiture procedures in the U.S. if such transactions are reported to or detected by the U.S. authorities (irrespective of whether the funds are denominated in Euros and kept out of the U.S. clearing sphere). This is due to the legal fiction employed by U.S. authorities according to which such funds are assumed to have been deposited in a correspondent account held in the U.S.

To avoid the outlined issues and mitigate the risks, EU banks have increasingly embarked on a policy of introducing contractual safeguards in connection with transactions involving risky counterparties. The safeguards consist mainly of contractual clauses that explain to customers various risks and protective measures taken by the banks, including:

- The potential freeze, seizure, and legal risks faced by a customer insisting on a U.S. Dollar denominated transaction involving a counterparty identified as uncooperative by the U.S.;
- The indemnity of the financing EU bank against any liability charges brought forward by the customer in the event of a freeze or seizure of funds enforced by U.S. authorities in connection with U.S. Dollar denominated transactions involving U.S. blacklisted counterparties; and

- The right of the financing EU bank to have recourse to the customer's funds in the event of such an enforced freeze or seizure of the bank's funds maintained in its U.S. correspondent bank account that is related to the customer's transaction.

The inclusion of contractual safeguards is also necessary in order to prevent effectively civil law claims and lawsuits. In case of an asset freeze and seizure imposed by the U.S. government, an EU bank could be potentially confronted with liability issues if it is established that the bank, due to gross negligence, failed to inform its customer of the aforementioned risks associated with U.S. Dollar denominated transactions involving U.S. blacklisted counterparties.

Resolving Conflicts of Laws: The German Example

German banks, in cases of gross negligence, are liable for any resulting damages caused to their customers and other contractual partners who are party to a transaction pursuant to the general terms and conditions governing the business of savings banks and other banks (Allgemeine Geschäftsbedingungen Sparkassen[51]/Banken[52]). Liability charges could be also based on the German Civil Code (Bürgerliches Gesetzbuch, the "BGB"[53]), according to which a claim for compensation could be filed for dereliction of duties in connection with a nongratuitous contract for services or work. Additional claims could arise from special regulations governing transfer of funds[54] or demand deposit accounts.[55]

However, where banks have acted properly, the situation is somewhat different. Pursuant to said AGB-Banken[56] and AGB-Sparkassen,[57] banks are not liable for events that are beyond their control. Asset freeze or seizure orders enforced by foreign third-country (i.e., non-EU) government authorities in their jurisdictions (e.g., under the USA PATRIOT Act regime) would constitute such an event. Although the use of a force majeure-based exemption clause has, in this context, given rise to various other issues concerning legal definition and interpretation, this instrument has been traditionally regarded by practitioners in Germany to provide some degree of legal relief. Moreover, it should be noted that the German Civil Code also contains exemption clauses with regard to the transfer of

funds[58] or demand deposit accounts[59] that refer to force majeure-type events.

The above issues were the subject of frequent discussions between German banking associations[60] and officials of the DoT in 2005 and 2006. The discussions additionally focused on the following procedural aspects of the U.S. AML regime relating to seizures and other enforcement actions where clarifications were requested:

- According to the DoT the number of cases where measures pursuant to Section 319(a) USA PATRIOT Act have been actually applied against banks since its enactment is very limited. The risk of applying this measure against EU banks is, moreover, reduced if a Mutual Legal Assistance Treaty (MLAT) exists between the US and the EU Member State in which a bank is headquartered.[61]
- The responsibility for authorizing legal actions lies with the United States Department of Justice, which maintains a robust legal and procedural framework. This includes the right of banks and targeted persons to lodge appeals with the courts in the U.S. However, the risk of application against an EU bank could not be limited to (1) cases where the targeted client of the bank is a national of a country that has no MLAT with the U.S. or (2) jurisdictions that have no MLAT with the U.S.
- Pursuant to DoT Section 319(a), measures would not be linked to U.S. sanctions and AML provisions that are applied only to non-U.S. banks within the territory of the U.S., such as OFAC sanctions, measures under Section 311 USA PATRIOT Act, and the Executive Order against Weapons of Mass Destruction (WMD) Proliferators and their Supporters.
- From the EU perspective, however, Section 319(a) measures would not allow a bank operating under the law of an EU Member State to recover any U.S. funds that had been seized from the bank's US correspondent account from its client (the supposed target of the seizure). Moreover, the German banking associations have pointed out that Section 319(a) seizures and the possibility of lodging subsequent

appeals with US courts should not replace regular procedures bilaterally agreed and established by governments under international law that also include the use of MLAT to resolve such issues. To that end the German banking sector has, as part of the EU financial industry, continued expressing a strong interest in obtaining clarification from the U.S. government that Section 319(a) measures would not be taken against EU banks or, at least, a clear definition of the circumstances under which such measures could be applied against EU banks.

- With respect to the finalized measures under Section 311 USA PATRIOT Act, and the Executive Order against WMD Proliferators and their Supporters, the DoT indicated the following:
  - The finalized measures under Section 311 USA PATRIOT Act, and the WMD-Executive Order apply to international banks' U.S. offices only.
  - Section 311 designations of financial institutions or jurisdictions as being of primary money laundering concern as well as proposed rulemakings under Section 311 would not oblige banks in the U.S. to cut off their relationship with the respective financial institution or jurisdiction, but were intended to trigger some enhanced scrutiny.
  - EU banks or exporters that (1) are headquartered outside the U.S. jurisdiction, (2) deal with firms listed in the WMD Executive Order, and (3) operate in line with export control law regimes of the EU or its Member States would not be subjected to this executive order as long as the respective transactions did not touch U.S. territory.

In April 2006, the two German banking associations submitted, as agreed with the representatives of the DoT, a letter to the DoT in which the above findings and results were summarized. The letter also contained an explicit request for a DoT response providing confirmation or further clarification on the points listed above. Regrettably, the DoT has not yet responded.

Challenges in Coping with Home-Host Conflicts

Due to the expansive and, with regard to designations, unilateral nature of the framework of AML/CFT regulations and the "smart" financial sanctions regime, EU banks conducting business in the U.S. — many of them through state or federally chartered branches[62] — have to contend with inquiries launched by the authorities, correspondent banks, and other business partners related to the issue of compliance with the U.S. AML/CFT and financial sanctions regimes. In such cases, the U.S. branch of a EU bank must carefully determine whether:

- Providing answers to inquiries based on unilateral measures imposed by the host country (i.e., U.S.) government would fundamentally violate home country laws (i.e., privacy/data protection law, AML/CFT and financial sanctions, and other regulations of the EU or the Member State in which the EU bank is incorporated); and
- The scope of reporting should be confined to the activities at U.S. branch level or expanded to cover the entire U.S.-related international business operations of the parent institution.[63]

Therefore, EU banks that have substantial U.S. business interests and operate in the U.S. through branches must carefully balance competing interests while making determinations on the extent of disclosure needed to respond to the inquiries of U.S. authorities and financial institutions satisfactorily. On one hand, such banks run substantial risks of not complying fully with the legal requirements concerning AML/CFT and OFAC if they provide insufficient information related to their business transactions to the U.S. authorities. On the other hand, full compliance with U.S. law creates the risk of home country law violations. Notably, the EU and its Member States have enacted a range of legislative measures to protect the economic and privacy interests of citizens and persons domiciled in the EU against measures unilaterally imposed by third countries and to penalize those economic operators within the EU or its Member States who support such measures.

Countermeasures of the EU — The Anti-Boycott Regulation

A prominent example of these protective measures is the Anti-Boycott Regulation of the EU.[64] This regulation provides protection against, and counteracts the effects of, the extra-territorial application of laws unilaterally adopted by third countries specified in an annex, including regulations and other legislative instruments, and of actions based thereon or resulting therefrom. The regulation is designed to safeguard the interests of natural persons resident in and legal persons (including EU banks) incorporated within the Community engaging in international trade and/or the movement of capital and related commercial activities between the Community and third countries, especially where such interests could be negatively affected by extra-territorial measures. The EU Anti-Boycott Regulation is a response to the Helms-Burton Act[65] and the Iran and Libya Sanctions Act of 1996,[66] which are unilateral U.S. measures aimed at sanctioning Cuba, Iran, and Libya and designed to have extra-territorial reach.[67] Due to political concerns, however, the EU Anti-Boycott Regulation does not list the USA PATRIOT Act in its annex of laws, regulations, and other legislative instruments. Accordingly, it cannot be invoked by EU banks as a protective countermeasure against demands of the U.S. authorities to comply with unilateral designations made under the USA Patriot Act (such as the designation concerning the Commercial Bank of Syria).[68]

Countermeasures of the EU-Member States

The dilemma is further compounded because some individual EU Member States (such as Germany) have legal provisions in force that categorically prohibit economic operators resident in their jurisdictions from supporting unilateral measures imposed by third countries. This is especially true in case of Section 4a of the German Foreign Trade Ordinance (Aussenwirtschaftsverordnung, "AWV"),[69] which explicitly prohibits residents of Germany from declaring their support for boycott measures adopted by a third country against another third country. Currently, Section 4a of the AWV is interpreted by the German government as a general provision requiring all economic operators to abstain from supporting unilaterally imposed Sanctions, Boycott, or Embargo measures that are

deemed to be disruptive to the principles of free international commerce and counterproductive to the foreign relations of Germany as a whole.[70] However, Section 4a of the AWV should not be construed as a provision designed generally to discourage economic operators from supporting sanctions imposed on the basis of international law. The German Foreign Trade Act (Aussenwirtschaftsgesetz — AWG)[71] which as an Act ranks higher than the AWV (which is an ordinance) is explicitly supportive of multilateral sanctions adopted by the U.N.

In view of the aforementioned and especially after the 9/11 attacks, EU banks frequently receive inquiries from U.S. authorities, correspondent banking institutions, and credit card issuing companies requesting details related to the status of their compliance concerning U.S. AML/CFT provisions (especially Section 311 USA PATRIOT Act) and OFAC designations. Given the anti-boycott regulation framework in the EU and its Member States as well as the larger political implications of the issue, EU banks have referred such cases to their home country supervisory authorities and requested clarification as to whether such inquiries from U.S. institutions could be answered on the basis of home country law. As an example, EU banks have been particularly careful not to include clauses in letters of credits requesting information from the beneficiaries regarding their business relationships with persons or institutions in third countries who have been unilaterally sanctioned/designated by the U.S. authorities. In Germany, for instance, answering such requests would be clearly regarded as a violation of national law (Section 4a AWV) and entail serious penalties (up to 500,000 Euro).[72]

Resolving Privacy and Data Protection Issues after the "SWIFT Controversy"

As previously discussed, the revelation in June 2006 of the U.S. government's confidential surveillance, through OFAC, of data handled by SWIFT caused considerable outrage in Europe.[73] As a result, the national data protection authorities of the EU Member States — backed by the European Commission — called upon the banking industry in their respective jurisdictions in June 2006 to take corrective actions by September 1, 2007.[74] In Germany, for example, the data protection authorities of the states (Länder)

issued a guidance indicating that merely posting customer information on the Internet homepages of banks or providing such information to customers on demand would be regarded as insufficient.[75] In the opinion of the German data protection authorities, the proactive provision of information by banks to customers (originating cross-border transfers of funds and flash payments) is deemed to be an appropriate policy approach to resolve the privacy issue arising from the SWIFT controversy. Therefore, German data protection authorities at state level are currently preparing further guidance on harmonized transparency obligations concerning customer information. The German banking industry has expressed its concerns regarding the approach favored by the authorities and has argued that the excess administrative burden for banks resulting from a proactive customer information policy far outweighs the benefits due to the very small share of affected customers involved in cross-border transactions. The German banking industry is, therefore, discussing an amendment to the terms and conditions governing the transfer of funds that would include a reference to the possible transfer of personal data to third countries (i.e., the U.S.) for CFT purposes.

Parallel to the discussions within the EU Member States, the European Commission and the EU Council Presidency have jointly undertaken substantial efforts to resolve the SWIFT controversy with the U.S. government. Following this joint undertaking, the EU received a set of unilateral commitments ("Representations") of the DoT regarding their handling of EU originating personal data received from SWIFT in the U.S. under compulsion of administrative subpoenas.[76] The DoT finalized the text of the Representations following discussions between the DoT and the Council Presidency and the European Commission. In the opinion of the European Commission, the Representations take account of EU concerns about the protection of EU originating personal data that may be subpoenaed in the United States by the DoT under its TFTP initiative. The Representations include the following important safeguards:

- Commitments by the DoT to use any data received from SWIFT exclusively for counterterrorism purposes — an obligation that applies also where such data are shared with other U.S. agencies and with third countries.[77]

- The DoT commits to analyse data subpoenaed from SWIFT on an ongoing basis in order to identify and delete any data which are not necessary for counter terrorism investigation.
- The Representations impose strict data retention obligations, namely to retain dormant data (i.e. data subpoenaed by the DoT which have not been identified as necessary for counter terrorism purposes) *for no more than five years from the date of receipt of data* or, in the case of data received before publication of the Representations, to retain those data *for no more than five years from the date of publication of the representations.*[78]
- The Representations further provide for appointment of an "*eminent European*" who will carry out annual oversight of the DoT's commitments contained in the Representations. The eminent person will be appointed by the Commission in consultation with the President of the Committee of Permanent Representatives and of the European Parliament's Civil Liberties Committee. The eminent person will report to the European Commission, which will report to Parliament and Council.
- To ensure transparency and legal certainty, the Representations, together with U.S. and EU letters of transmission and receipt, have been published in the Official Journal of the European Union in all official languages.[79] In the United States the DoT will endeavour to ensure publication of the Representations in the U.S. Federal Register.

The Representations constitute one of three main components of the measures to address the infringement of European data protection law due to SWIFT's transfer of data to the U.S. and possible access to some of those data by the DoT under the TFTP. To make lawful the transfer of SWIFT data for commercial purposes to its server in the United States, SWIFT is in the final stages of discussions with U.S. authorities regarding entry into the "Safe Harbor."[80] SWIFT and the financial institutions that use SWIFT's services are working to ensure that bank customers will be properly informed, including that their personal data will be transferred to the U.S. and could be accessed by DoT under the TFTP. The EU letter

of reply to the DoT notes that, if the necessary information obligations are met by SWIFT and the financial institutions that use its services, and if SWIFT respects the Safe Harbor principles, SWIFT and the financial institutions that use its services will be in compliance with their respective obligations under European data protection law. The European Commission considers that the legal framework resulting from the above-mentioned elements is sufficient to guarantee respect for and the enforcement of European data protection rights.

CONCLUSION

The provisions of the USA PATRIOT Act affecting foreign banks largely center around correspondent account transactions and clearing issues, as well as home and host country compliance conflicts resulting from significant differences between EU and U.S. boycott and data protection regimes. Foreign banks wishing to maintain correspondent accounts should be prepared to comply with increased due diligence. Home-jurisdiction regulations and the in-house policies of foreign banks can, however, impact the nature of the diligence procedures of U.S. banks. Furthermore, stringent provisions can prevent foreign jurisdictions and institutions from being subject to special measures that would require even more intrusive review.

Perhaps more troubling, foreign banks may be subject to U.S. government subpoenas and seizures of funds held in interbank accounts. The USA PATRIOT Act has significantly increased the tools available to U.S. authorities seeking information about terrorist and money laundering activity. After almost seven years, much still remains to be seen about the actual effectiveness of these provisions in fighting money laundering and terrorist financing. Although controversies are beginning to arise, courts have yet to provide insight into the interpretation and enforcement of the new laws.

Internationally active EU banks that have substantial business interests in the U.S. and operate in the U.S. through branches face difficult decisions and serious risks. So long as U.S. authorities continue to enforce PATRIOT Act provisions, the challenge for EU banks will be to confine their U.S. reporting and compliance obligations to their local

branches with regard to transactions that involve U.S. counterparties and are sourced in the U.S. so that tensions between the laws of the EU and its Member States are minimized. This strategy certainly poses substantial challenges for the compliance and risk management process of EU banks on a group-wide basis.

EU banks are willing to comply with the requirements of the U.S. AML/CFT and financial sanctions regimes to a reasonable extent. EU banks, after all, are required by their respective home country regulations to rigorously implement AML/CFT standards of the FATF and the financial sanctions of the UN.[81] Moreover, a number of EU and other foreign banks seeking to expand their business interests further in the U.S. due to the attractive opportunities and returns offered by the banking market have launched initiatives to create an atmosphere of trust and goodwill by updating the compliance systems of their U.S. operations and by voluntarily terminating their business relationships with counterparties in third countries sanctioned or designated by the U.S. authorities.[82] Nonetheless, there is also considerable frustration within the international and EU banking community concerning overregulation in the area of AML/CFT regulation, which, together with the Sarbanes Oxley legislation, the CFIUS legislation currently discussed in the U.S. Congress, and the recent decision by the Securities and Exchange Commission (SEC) to add to its Web site a link to a list of predominantly non-US companies that have some minimal business dealings with so-called "State Sponsors of Terrorism,"[83] could severely erode the international standing and competitiveness of U.S. financial centers such as New York and tarnish the image of the U.S. as an open and liberal economy.[84]

NOTES

[1] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub L. No. 107–56 (Oct. 26, 2001); *see also* Indranil Ganguli, EU-Finanzsanktionen — Eine praxisorientierte Einführung, Berlin 2006, 179-186.

[2] Exec. Order on Terrorist Financing of Sept. 24, 2001 (abbreviated: Terrorist Financing-Executive Order) and Exec. Order: Blocking Property of

Weapons of Mass Destruction Proliferators and Their Supporters of June 29, 2005 (abbreviated: WMD-Executive Order).

[3] See the official OFAC Web site, *at* http://www.treas.gov/offices/enforcement/ofac/ (last visited Sep. 12, 2007) for OFAC designations and the U.S. financial sanctions program/regime.

[4] It is important to bear in mind that the AML/CFT regime and the financial sanctions regime are closely interrelated and to a great extent interdependent (*see* Ganguli, *supra* note 1, at 16, 31-33, and 57-58). A detailed discussion of the interdependencies between OFAC designations and the financial sanctions regime of the U.S. government on the one hand and the USA PATRIOT Act on the other hand is beyond the scope of this article, as this article focuses on the currently applicable framework of the U.S. AML/CFT regulations.

[5] The case of the Dutch bank ABN Amro shows that in some instances such punitive/corrective measures are enforced by U.S. authorities on a group-wide basis covering all business lines and overseas locations of a foreign banking institution. *See The Federal Reserve Board, Agencies release bank supervisory and penalty actions against ABN AMRO Bank, N.V.*, Joint Press Release Dec. 19, 2005.

[6] However, it should be noted that the presentation and analysis of issues and challenges facing EU banks were mostly drawn from the experience of internationally active banks headquartered in the EU Member State of Germany as Mr. Ganguli has considerable expertise in dealing with the European and German aspects of the issues.

[7] Michael Gruson, *The US Jurisdiction over Transfers of U.S. Dollars Between Foreigners and over Ownership of U.S. Dollar Accounts in Foreign Banks*, 3 Colum. Bus. L. Rev. 735 (2004).

[8] For further details and implications of the SWIFT controversy, *see infra.*

[9] Ganguli, *supra* note 1, at 181-82.

[10] For data security reasons, SWIFT operates two identical "mirror" servers, one located in the EU and the other in the U.S. All financial messaging data are held on each server for a period of 124 days.

[11] Commission de la Protection de la Vie Privee, Opinion on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC) Subpoenas, Sept. 27, 2006.

[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Official Journal of

the EU L 281, 23. Nov. 1995, 31–50 (abbreviated: EU-Data Protection Directive).

[13] The panel is known as the Article 29 Working Party, which acts as an independent advisory body to the European Commission; *see* European Commission, The SWIFT case and the American Terrorist Finance Tracking Program, MEMO/07/266, Brussels, 28 June 2007 (abbreviated: MEMO/07/266) *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/266&format=HTML&aged=0&language=EN&guiLanguage=en (last visited Sep. 12, 2007)).

[14] Eric Lichtblau, *Europe Panel Faults Sifting of Bank Data*, N.Y. Times, Sept. 26, 2006; *see also* MEMO/07/266.

[15] It is worth noting in this context that as a result of the controversy SWIFT has recently made a public announcement stating its intent to remedy the situation by addressing the compliance issues (*see* M. Kurm-Engels, *Swift will Daten besser schützen*, Handelsblatt, Apr. 2, 2007). According to the quoted newspaper article SWIFT has promised to (a) further enhance contractual compliance and transparency, where appropriate, of the processing of (personal) message data, (b) take steps to adhere to the safe harbor framework of EU privacy/data protection regulations and (c) develop business cases for improving its current global architecture (e.g. technical processing, including locations and facilities of networks and data centers).

[16] Branches of foreign banks operating within the United States are subject to federal and, in many cases, state regulation. Under the terms of the USA PATRIOT Act, foreign bank branches in the United States are subject to the USA PATRIOT Act in the same manner as domestic banks.

[17] 31 U.S.C. § 5318(i)(1) (2007).

[18] 31 C.F.R. § 103.176 (2007).

[19] 67 Fed. Reg. 37743 (May 30, 2002).

[20] 31 U.S.C. § 5318A(e)(1)(B); 31 C.F.R. § 103.175 (2007).

[21] 31 C.F.R. § 103.76(a).

[22] 31 U.S.C. § 5318A.

[23] The FATF is an intergovernmental body charged with setting AML standards, which are today widely accepted by the G8 countries and Member States of the Organization for Economic Co-operation and Development (OECD) as well as other major emerging market nations.

[24] A number of countries were once deemed to be NCCTs, including several on the fringe of Europe. With the removal of Myanmar in October 2006 the

"blacklist" does not contain any designated countries. Member States of the EU should be aware, but generally feel safely beyond the reach, of this designation. For more information on the background and development of the NCCT initiative, *see* the FATF homepage *at* http://www.fatf-gafi.org/document/4/0,2340,en_32250379_32236992_33916420_1_1_1_1,00.html (last visited Sep. 12, 2007).

[25] 31 C.F.R.§ 103.76(b).

[26] 31 U.S.C. § 5318A.

[27] 31 U.S.C. § 5318A(b).

[28] 31 U.S.C. § 5318A(c).

[29] Regulation (EC) No. 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community, Official Journal of the EU L 309, 25 Nov. 2005, 9-12 (abbreviated: EU-Cash Control Regulation).

[30] 31 U.S.C. § 5318(j).

[31] 31 C.F.R. § 103.177.

[32] Gruson, *supra* note 7, at 722; *see also* Cortright et al., *Targeted Financial Sanctions: Smart Sanctions That Do Work, in Targeting Economic Statecraft*, 23-40 (2002).

[33] 18 U.S.C. § 1956(b).

[34] 31 U.S.C. § 5318(k)(3).

[35] 18 U.S.C. § 981(k).

[36] Gruson, *supra* note 7, at 756.

[37] 18 U.S.C. § 983(k).

[38] Gruson, *supra* note 7, at 749-56.

[39] The case of the Dutch bank ABN AMRO and the Swiss bank UBS demonstrates the determination of U.S. authorities to exercise their powers to penalize foreign banks deemed to have violated U.S. AML laws and the extent to which the U.S. authorities will go in obtaining sanctions against such foreign banks. *See* The Federal Reserve Board, *Agencies release bank supervisory and penalty actions against ABN AMRO Bank, N.V.*, December 19, 2005, available at http://www.federalreserve.gov/BoardDocs/Press/enforcement/2005/20051219/default.htm (last visited Sep. 12, 2007) and
The Federal Reserve Board, *Order of assessment of a civil money penalty [against UBS AG] May 10, 2004, available at* http://www.federalreserve.gov/boarddocs/press/enforcement/2004/200405102/default.htm (last visited Sep. 12, 2007).

[40] 12 U.S.C. § 1828(c).
[41] Title III, Section 353(a) and (b).
[42] 12 U.S.C. § 1953.
[43] 12 U.S.C. § 1829b.
[44] Title III, Section 353(d).
[45] 31 U.S.C. § 5321(a) was amended by appending Section 7.
[46] 31 U.S.C. § 5322.
[47] So defined in 31 U.S.C. § 5318(i) and 31 U.S.C. § 5318(j), as well as in special measures imposed under 31 U.S.C. § 5318A.
[48] The USA PATRIOT Improvement and Reauthorization Act of 2005, which extends the duration of the USA PATRIOT Act, the speech of President George W. Bush of July 20, 2005 on the importance of the USA PATRIOT Act, and the remarks of Governor Schmidt Bies on March 14, 2005 highlighting AML issues from a banking supervisory perspective substantiate this assumption to a very great extent (Title of President Bush's speech: *"United States Fighting Terror by Going on Offensive," available at* http://amerikadienst.usembassy.de (last visited Sep. 12, 2007) and title of Governor Schmidt Bies' remarks: *"Bank Secrecy Act and capital compliance issues"* — Remarks by Ms Susan Schmidt Bies, Member of the Board of Governors of the US Federal Reserve System, at the Institute of International Bankers Annual Washington Conference, *available at* http://www.bis.org/review/r050321h.pdf (last visited Sep. 12, 2007)).
[49] Privacy/data protection issues surfaced during the SWIFT controversy in such a contentious manner that the EU institutions and the U.S. government had to resort to diplomatic means to resolve the conflict.
[50] *See* Ganguli, *supra* note 1, at 183.
[51] Allgemeine Geschäftsbedingungen Sparkassen (AGB-Sparkassen), *available at* http://www.berliner-sparkasse.de/module/static/agb/agb.pdf?IFLB-SERVERID=IF@@103@@IF (last visited Sep. 12, 2007).
[52] Allgemeine Geschäftsbedingungen Banken (AGB-Banken), *available at* http://www.bankenverband.de/pic/artikelpic/052004/ge0405_re_AGB.pdf (last visited Sep. 12, 2007).
[53] § 280 BGB in connection with § 675 BGB.
[54] § 676a BGB.
[55] § 676f BGB.
[56] No. 3 paragraph 3 AGB-Banken.
[57] No. 19 paragraph 3 AGB-Sparkassen.

[58] § 676b sub-paragraph 4 BGB.
[59] § 676g sub-paragraph IV sentence 6 BGB.
[60] Bundesverband Öffentlicher Banken Deutschlands (Association of German Public Sector Banks) and Bundesverband Deutscher Banken (Association of German Banks — private sector banks).
[61] The United States has signed MLATs with the EU (on June 25, 2003) and a number of its Member States, inter alia Germany (on October. 14, 2003). However, the treaties with the EU and Germany have not yet entered into force (*see* http://travel.state.gov/law/info/judicial/judicial_690.html (last visited Sep. 12, 2007)).
[62] U.S. Branches of EU banks — as opposed to subsidiaries — face the problem that they, along with their parent EU bank and its other affiliates, are supervised on a consolidated basis by the EU bank's home country authorities, while the U.S. branches must also comply with host country standards and regulations to the extent that their business is sourced in or related to their host country jurisdiction.
[63] In the latter case, it is recommended to process the inquiry at the headquarter of the parent institution.
[64] Council Regulation (EC) No 2271/96 of 22 Nov. 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom; Official Journal of the EU L 309, 29. Nov. 1996, 1-6 (abbreviated: EU-Anti-Boycott Regulation).
[65] Also known as *Cuban Liberty and Democratic Solidarity Act of 1996*.
[66] *See* annex of EU-Anti-Boycott Regulation.
[67] For further details, *see also* Hocke, Ernst et al., *Aussenwirtschaftsrecht — Gesetze, Verordnungen und Erlasse zum Aussenwirtschaftsrecht mit Kommentar* (abbreviated: Hocke et al.), R. v. Decker Verlag Heidelberg 2005, Ordner 1, Hauptteil I, 3. Teil, at 23.
[68] *See* U.S. DoT, *Treasury Designates Commercial Bank of Syria as Financial Institution of Primary Money Laundering Concern — 311 Action Comes on the Heels of President Bush's Declaration of National Emergency with Respect to Syria*, May 11, 2004, *available at* http://www.treas.gov/press/releases/js1538.htm (last visited Sep. 12, 2007).
[69] *Verordnung zur Durchführung des Aussenwirtschaftsgesetzes [Aussenwirtschaftsverordnung* — abbreviated: AWV], Bundesgesetzblatt (BGBl.) I 1986, 2671, neugefasst durch Bekanntmachung vom 22.11.1993 BGBl. I 1934, 2493, zuletzt geändert durch Art. 2 Gesetz v. 28.03.2006

BGBl. I S. 574; Ausfuhrliste neugefasst durch Verordnung v. 29.04.2005 Bundesanzeiger Nr. 85, 7117 and Hocke et. al, Ordner 1, Hauptteil I, 3. Teil, at 23 as well as Ordner 1, Hauptteil II, 4. Teil, § 4a AWV (Kommentar), at 1-4. This provision was introduced in 1992 as a countermeasure to pressures exerted by some Arabian countries on German exporters demanding a declaration/assurance (to be submitted with the commercial invoice and the certificate of origin) that the German goods exported to those countries were not produced in Israel or did not contain components originating from Israel prior to their exportation.

[70] *See* Hocke et al., Ordner 1, Hauptteil I, 1. Teil, (Wortlaut) at 5; *see also* Ordner 1, Hauptteil II, 4. Teil, § 4a (Kommentar), at 1.

[71] *Aussenwirtschaftsgesetz* (AWG), BGBl. I 1961, 481, 495, 1555, zuletzt geändert durch Art. 1 Gesetz v. 28.3.2006, BGBl. I S. 574; Einfuhrliste neugefasst durch Verordnung vom 19.12.2005, BAnz. Nr. 248, 17325; *see also* Hocke et al., Ordner 1, Hauptteil I, 3. Teil, § 1 AWG (Kommentar), at 5, § 5 AWG (Kommentar), at 1-5; *see also* Hocke et al., Ordner 1, Hauptteil II, 4. Teil, § 4a AWV (Kommentar), at 1-2.

[72] § 70 subparagraph 1 no. 1 and § 33 (AWG); *see also* Hocke et al., Ordner 1, Hauptteil II, 4. Teil, § 4a (Kommentar), at 4. If a violation is construed to be sufficiently severe so as to endanger the principle of "peaceful coexistence of nations" enshrined in § 7 AWG and § 34 AWG prison sentences of up to five years might additionally apply; *see* Hocke et al., Ordner 1, Hauptteil II, 4. Teil, § 4a (Kommentar) at 4.

[73] *See* motion no. 16/4066 of the German Parliament dated Jan. 17, 2007 (*Deutscher Bundestag [BT], Antrag der Abgeordneten Omid Nouripour et. al. und der Fraktion BÜNDNIS 90/DIE GRÜNEN; SWIFT-Fall aufklären — Datenschutz im internationalen Zahlungsverkehr wieder herstellen; BT Drucksache 16/4066*).

[74] *See* MEMO/07/266.

[75] The guidance was issued in a letter of the Data Protection Authority of the State of Bremen (*Landesbeauftragter für Datenschutz und Informationsfreiheit, Freie Hansestadt Bremen*) dated Nov. 10, 2006 (reference file no. 11-500-01.06/3#48) on behalf of all German state data protection authorities. At the time of the SWIFT controversy, the Bremen authority presided over the panel of the German state data protection authorities (*"Düsseldorfer Kreis"*), which monitors compliance of the non-public sector with German data protection laws.

[76] European Commission, *USA to take account of EU data protection principles to process data received from Swift*, IP/07/968, Brussels 28 June 2007 (abbreviated: IP/07/968), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/968&format=HTML&aged=0&language=EN&guiLanguage=de) (last visited Sep. 12, 2007).

[77] Any other use of SWIFT data is therefore excluded, including, for example, use of those data for commercial or industrial purposes.

[78] This means, for example, that if the Representations are published on Sept. 1, 2007, data that might be received on Sept. 15, 2007 and that remain dormant would have to be deleted by no later than Sept. 15, 2012.

[79] *See* Official Journal of the EU C 166, 20 July 2007, 17-27.

[80] The Safe Harbor is a specific type of "Adequacy Decision" adopted by the European Commission in order to allow the free flow of personal data between the EU and the U.S. It allows EU controllers to export personal data to U.S. organizations that have joined the Safe Harbor, since the privacy principles it contains are recognized to afford the adequate protection required by the EU for international data transfers. The European Commission has declared in 2000 that the Safe Harbor offers an adequate level of protection in accordance with the EU-Data Protection Directive (Decision of July 26, 2000). Once a U.S. organization has self-certified and is admitted by the U.S. Department of Commerce as a member of the Safe Harbor, it is able to accept transfers of personal data lawfully processed in the EU. SWIFT anticipates that it will join the Safe Harbor by early July 2007 once the U.S. Department of Commerce has admitted and registered them as a member of the Safe Harbor. The Safe Harbor allows limitations on its data protection principles for important public purposes: "to the extent necessary to meet national security, public interest or law enforcement requirements." In this respect, it is necessary to show that the processing by the U.S. of EU originating personal data is necessary, proportionate, and in compliance with European data protection law. This is precisely the aim of the Representations.

[81] Directive 2005/60/EC of the European Parliament and of the Council of 26 Oct. 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing; Official Journal of the EU L 309, 25 Nov. 2005, 15-36 and Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 Nov. 2006 on information on the payer accompanying transfers of funds; Official Journal of the EU L 345, 8 Dec. 2006, 1-9. Both legislative measures of the EU implement the FATF-

40+9 Recommendations into Community law. UN financial sanctions transposed into Community law, *available at* http://ec.europa.eu/comm/external_relations/cfsp/sanctions/measures.htm (last visited Sep. 12, 2007).

[82] The decision of the Swiss banks UBS and Credit Suisse (*see* Article titled *Rückzug aus dem Irangeschäft*, Handelsblatt, Feb. 2, 2006) as well as the German Commerzbank (*see* Article titled *USA drängen deutsche Firmen aus dem Iran*, Jan. 11, 2007) to terminate their business relationships with Iran is indicative of the new international strategy of many EU-based banks aimed at improving their image and stature on the U.S. markets as well as their standing with the U.S. supervisory agencies.

[83] The SEC added the link to its Web site on June 25, 2007. SEC's action triggered massive criticism from domestic and international public opinion that the listings have been compiled without regard to the content of the company's disclosure or its materiality and that the result is needlessly provocative and contrary to the desire to promote the U.S. capital markets abroad. Following this criticism SEC Chairman Cox announced on July 20, 2007 the removal of the "State Sponsors of Terrorism" link from the SEC's Web site pending consideration of alternative means to communicate to investors information regarding the extent of listed companies' activities in countries designated by the State Department as "State Sponsors of Terrorism" (*see* letter of Congressman Barney Frank *available at* http://www.iib.org/associations/6316/files/20070712FrankLetter.pdf (last visited Sep. 12, 2007); Jeremy Grant, *Banks urge SEC to remove 'terror' web links*, Fin. Times, July 10, 2007; SEC press release of June 25, 2007 *available at* http://www.sec.gov/news/press/2007/2007-121.htm (last visited Sep. 12, 2007) and SEC press release of July 20, 2007 *available at* http://www.sec.gov/news/press/2007/2007-138.htm (last visited Sep. 12, 2007)).

[84] The McKinsey study commissioned by Mayor Bloomberg and Senator Schumer of January 2007 provides valuable insights into this issue and contains a clear warning that New York is in danger of losing its status as a global financial market without a major shift in U.S. regulations and public policy (the complete study is *available at* http://www.nyc.gov/html/om/pdf/ny_report_final.pdf (last visited Sep. 12, 2007)).